

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-154976

(43) 公開日 平成10年(1998) 6月9日

(51) Int.Cl.⁵

H 0 4 L 9/10

識別記号

F I

H 0 4 L 9/00

6 2 1 A

6 2 1 Z

審査請求 未請求 請求項の数11 O L (全 15 頁)

(21) 出願番号 特願平8-311924

(22) 出願日 平成8年(1996)11月22日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 清水 秀夫

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(72) 発明者 新保 淳

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(72) 発明者 川村 信一

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

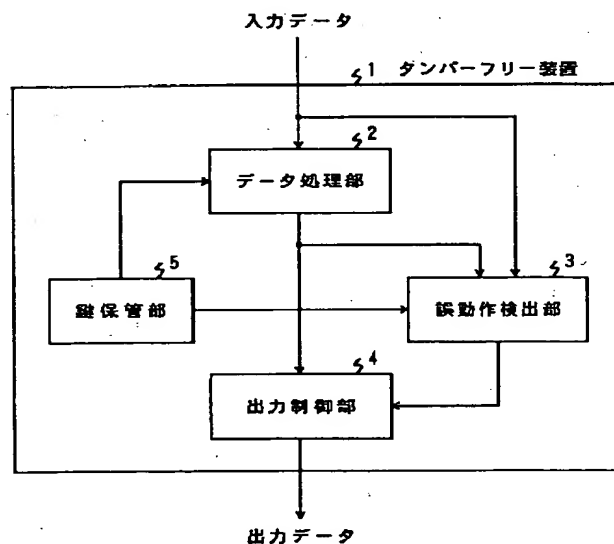
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 タンパーフリー装置

(57) 【要約】

【課題】 外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を推測する攻撃法に対して防御可能なタンパーフリー装置を提供することを目的とする。

【解決手段】 内部に外部からの入力データに対して所定のデータ変換処理を施して出力するための手段を備え、内部情報への不正アクセスを防止するために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、前記データ変換処理の誤動作を検出する手段と、誤動作が検出された場合に前記処理の出力に所定の規制を施す出力規制手段とを備えたことを特徴とする。



1

【特許請求の範囲】

【請求項1】 内部に外部からの入力データに対して所定のデータ変換処理を施して出力するための手段を備え、内部情報への不正アクセスを防止するために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、

前記データ変換処理の誤動作を検出する手段と、誤動作が検出された場合に前記処理の出力に所定の規制を施す出力規制手段とを備えたことを特徴とするタンパーフリー装置。

【請求項2】 入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、入力データに対して鍵情報を用いた所定のデータ変換処理を施す手段と、

前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記所定のデータ変換処理において誤動作が発生したか否かを検出する手段と、この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とするタンパーフリー装置。

【請求項3】 入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、予め定められた、鍵情報を用いて行う複数種類のデータ変換処理のうち実行すべきもの指示する情報を入力する手段と、

入力データに対して、指示されたデータ変換処理を施す手段と、

前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記データ変換処理において誤動作が発生したか否かを検出する手段と、この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とするタンパーフリー装置。

【請求項4】 入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、予め定められた、複数の鍵情報のうち使用すべきもの指示する情報を入力する手段と、

2

入力データに対して、指示された前記鍵情報を用いた所定のデータ変換処理を施す手段と、

入力データに対して、指示されたデータ変換処理を施す手段と、

前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記データ変換処理において誤動作が発生したか否かを検出する手段と、

この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とするタンパーフリー装置。

【請求項5】 前記検出する手段は、前記入力データに対して、前記所定のデータ変換処理と同一の処理を施し、得られた結果が前記所定のデータ変換処理により得られた結果と一致するか否かによって、誤動作が発生したか否かを検出することを特徴とする請求項1ないし4のいずれか1項に記載のタンパーフリー装置。

【請求項6】 前記データ変換処理を施す手段における前記データ変換処理を行う回路と、前記検出する手段における前記処理を行う回路とを、同一半導体基板上で距離を離して設けたことを特徴とする請求項5に記載のタンパーフリー装置。

【請求項7】 前記検出する手段は、前記データ変換処理の結果得られたデータに対して、前記所定のデータ変換処理の逆変換処理を施し、得られた結果が前記入力データと一致するか否かによって、誤動作が発生したか否かを検出することを特徴とする請求項1ないし4のいずれか1項に記載のタンパーフリー装置。

【請求項8】 前記データ変換処理と前記逆変換処理とをパイプライン的に並列動作させるようにしたことを特徴とする請求項7に記載のタンパーフリー装置。

【請求項9】 暗号アルゴリズムが積暗号である場合、各ラウンド処理毎に前記誤動作の検出を行うようにしたことを特徴とする請求項1ないし4のいずれか1項に記載のタンパーフリー装置。

【請求項10】 入力データに所定のデータ変換処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、

前記所定のデータ変換処理が準同型性を持つ場合、入力データに乱数を混入させたものに対して該データ変換処理を施し、得られた結果から、該乱数の影響を取り除いて、出力することを特徴とするタンパーフリー装置。

【請求項11】 前記所定のデータ変換処理は、暗号化処理、復号化処理、デジタル署名、またはデジタル署名の署名検証であることを特徴とする請求項1ないし10のいずれか1項に記載のタンパーフリー装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、放射線や他の物理手段により誤動作を生じさせ内部に封入された秘密を分解せずに暴こうとする攻撃に対して安全なタンパーフリー装置に関する。

【0002】

【従来の技術】現在、コンピュータや記憶装置あるいは通信網など、情報を電子化して処理、保存、通信などする技術がかなり高度化されるとともに、ますます研究開発が盛んになってきている。また、このような技術は、実際に、様々な分野において様々な形で利用されている。中でも、情報を第3者から秘匿した状態で蓄積や転送などするための基盤技術である暗号技術の重要性は非常に高まっており、盛んに研究開発が行われているとともに、電子課金の情報、機密情報、著作権に係る情報あるいはプライバシーに関する情報などを扱うシステムに実際に利用されている。

【0003】暗号技術を研究開発する場合、主に新たな暗号方式を提供するだけではなく、その新たな暗号方式における暗号解読の困難性を検証することも重要なテーマである。しかして、従来は、暗号解読は通信路の盗聴を前提としており、暗号化や復号を行う装置自体は、安全であって危険にさらされることはない、という前提があった。特に、例えばICカードのように、分解や走査されることにより内部の情報を読み取ることを困難にしたタンパーフリー装置（タンパーブルーフ装置あるいはタンパーレジスト装置とも呼ばれる）は、鍵の安全な保管装置としてだけではなく、計算能力（CPU）も封入することで、鍵を外部に知られることなく、暗号化、復号化、認証処理などのデータ処理が可能な、安全なデータ処理装置を構成できるものと考えられていた。なお、タンパーフリー装置については、例えば、「Super distribution : The Concept the Architecture」、Masaji Kawahara、THE TRANSACTION OF THE IEICE、Vol. E73、No. 7、JULY 1990に開示されている。

【0004】ところが、BransonやLindstromは、タンパーフリー装置を分解や操作することなく、内部の秘密情報を暴く新しい暗号解析技術を提示した（例えば、インターネットにおける“http://www.bellcore.com/PRESS/ADVSRY96/facts.html”）。その技術は、タンパーフリー装置に外部から放射線や電子、熱や振動など物理的な衝撃を加え、内部装置を誤動作（内部のレジスタが1bit反転する）させ、誤動作の結果得られた出力データを幾つか蓄積し、これら出力データに与えた誤動作の影響の仕方を観察することにより、内部

情報を推測するというものである。このような技術は、これまでは想定されていなかったもので、ICカードのようなタンパーフリーな暗号装置を利用者が手軽に利用できるようになったという社会背景と、暗号装置自身は攻撃されないことを前提としてきた従来の研究開発の指針とを考慮すると、既存の概念にある程度の転換を迫るものと言える。

【0005】BihamとShamirも同じ原理に基づいてDESのようなブロック暗号を解読する方法を提案した（例えば、インターネットにおける“http://www.CS.tecnion.ac.il/~biham/dfa.html”）。計算機によるシミュレーションの結果、この方法によれば、例えば約200個程度の出力データの観察によりDESの56bitの鍵を手に入れることが可能であることが示されている。

【0006】

【発明が解決しようとする課題】従来のタンパーフリー装置は、外部から放射線や電子、熱や振動などの物理的衝撃を加えることによって暗号化回路などの内部回路を誤動作させ、誤動作の反映された出力データを蓄積し観察することによって内部の秘密情報を推測する新しい暗号解読法に対して、対策が施されていないという問題があった。

【0007】本発明は、上記事情を考慮してなされたもので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を推測する攻撃法に対して防御可能なタンパーフリー装置を提供することを目的とする。

【0008】

【課題を解決するための手段】本発明（請求項1）は、内部に外部からの入力データに対して所定のデータ変換処理を施して出力するための手段を備え、内部情報への不正アクセスを防止するために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、前記データ変換処理の誤動作を検出する手段と、誤動作が検出された場合に前記処理の出力に所定の規制を施す出力規制手段とを備えたことを特徴とする。

【0009】本発明によれば、タンパーフリー装置の内部回路が誤動作した場合、処理結果のデータ出力に所定の規制を施すので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【0010】本発明（請求項2）は、入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、入力データに対して鍵情報を用いた所定のデータ変換処理を施す手段と、前記入力データおよび前記所定のデータ変換処理により得られたデータ

5

をもとにして、前記所定のデータ変換処理において誤動作が発生したか否かを検出する手段と、この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とする。

【0011】本発明によれば、タンパーフリー装置の内部回路が誤動作した場合、処理結果をデータ出力しないので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【0012】本発明（請求項3）は、入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、予め定められた、鍵情報を用いて行う複数種類のデータ変換処理のうち実行すべきもの指示する情報を入力する手段と、入力データに対して、指示されたデータ変換処理を施す手段と、前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記データ変換処理において誤動作が発生したか否かを検出する手段と、この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とする。

【0013】本発明によれば、タンパーフリー装置の内部回路が誤動作した場合、処理結果をデータ出力しないので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【0014】本発明（請求項4）は、入力データに所定の処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、予め定められた、複数の鍵情報のうち使用すべきもの指示する情報を入力する手段と、入力データに対して、指示された前記鍵情報を用いた所定のデータ変換処理を施す手段と、入力データに対して、指示されたデータ変換処理を施す手段と、前記入力データおよび前記所定のデータ変換処理により得られたデータをもとにして、前記データ変換処理において誤動作が発生したか否かを検出する手段と、この検出の結果、前記所定のデータ変換処理において誤動作が発生したと判断された場合、前記所定のデータ変換処理により得られたデータを外部に出力させないように制御する手段とを備えたことを特徴とする。

【0015】本発明によれば、タンパーフリー装置の内

6

部回路が誤動作した場合、処理結果をデータ出力しないので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【0016】本発明（請求項5）は、請求項1ないし4のいずれか1項に記載のタンパーフリー装置において、前記検出する手段は、前記入力データに対して、前記所定のデータ変換処理と同一の処理を施し、得られた結果が前記所定のデータ変換処理により得られた結果と一致するか否かによって、誤動作が発生したか否かを検出することを特徴とする。

【0017】本発明（請求項6）は、請求項5に記載のタンパーフリー装置において、前記データ変換処理を施す手段における前記データ変換処理を行う回路と、前記検出する手段における前記処理を行う回路とを、同一半導体基板上で距離を離して設けたことを特徴とする。

【0018】本発明（請求項7）は、請求項1ないし4のいずれか1項に記載のタンパーフリー装置において、前記検出する手段は、前記データ変換処理の結果得られたデータに対して、前記所定のデータ変換処理の逆変換処理を施し、得られた結果が前記入力データと一致するか否かによって、誤動作が発生したか否かを検出することを特徴とする。

【0019】本発明（請求項8）は、請求項7に記載のタンパーフリー装置において、前記データ変換処理と前記逆変換処理とをパイプライン的に並列動作させるようにしたことを特徴とする。

【0020】これによって、誤動作検出処理に伴う処理時間の増大を防ぐことができる。本発明（請求項9）は、請求項1ないし4のいずれか1項に記載のタンパーフリー装置において、暗号アルゴリズムが積暗号である場合、各ラウンド処理毎に前記誤動作の検出を行うようにしたことを特徴とする。

【0021】これによって、誤動作検出処理に伴う処理時間の増大を防ぐことができる。本発明（請求項10）は、入力データに所定のデータ変換処理を施して外部に出力する機能を有し、外部から自装置内部に存在するデータにアクセスすることおよび外部から該機能を変更させることを不能とするために内部回路全体を物理的手段により外部から保護したタンパーフリー装置であって、前記所定のデータ変換処理が準同型性を持つ場合、入力データに乱数を混入させたものに対して該データ変換処理を施し、得られた結果から、該乱数の影響を取り除いて、出力することとを特徴とする。本発明によれば、計算途中で生じた誤動作の影響を直接出力データに反映させないようにすることができるので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【0022】本発明（請求項11）は、請求項1ないし

10

20

30

40

50

10のいずれか1項に記載のタンパーフリー装置において、前記所定のデータ変換処理は、暗号化処理、復号化処理、デジタル署名、またはデジタル署名の署名検証であることを特徴とする。

【0023】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。前述したように、例えばICカードなどのようなタンパーフリー装置に、外部から放射線や電子、熱や振動など物理的な衝撃を加え、内部装置を誤動作させ、誤動作の結果得られた出力データを幾つか蓄積し、これら出力データに与えた誤動作の影響を観察することにより、装置内部に隠された秘密情報を暴こうとする新しい暗号解析技術が知られている。

【0024】本実施形態は、概略的には、このような新たな攻撃方法に対処するために、タンパーフリー装置内で誤動作が生じた場合、内部情報の反映されたデータが外部に出力しないようにしたものである。

【0025】図1に、本発明の第1の実施形態に係るタンパーフリー装置の構成を示す。このタンパーフリー装置1は、例えばその内部回路を半導体集積装置により形成し、これを樹脂で封止するなどの対策を講じることにより、(1)外部から内部回路中に存在するデータをアクセス不可とし、かつ(2)外部から内部回路の機能を変更させることを不可とする。すなわち、外部からは、処理に必要なデータを入力することと、処理結果のデータを得ることしかできないものとする。なお、タンパーフリー装置1の内部回路は、ハード・ワイヤードで形成しても良いし、書き込み不能のROM回路に書き込んだプログラムをCPUで実行するような構成で形成しても良い。

【0026】図示はしていないが、タンパーフリー装置1の電源は、外部から供給するようにしても良いし、電池を内蔵しても良い。また、タンパーフリー装置1は、必要に応じて外部装置とのインターフェース手段を備えても良い。また、タンパーフリー装置1を外部装置に接続する端子には、種々のコネクタ類が使用可能である。なお、タンパーフリー装置1に無線通信手段を内蔵し、無線により接続しても良い。

【0027】さて、図1に示すように、このタンパーフリー装置1は、データ処理部2、誤動作検出部3、出力制御部4、鍵保管部5を備えている。データ処理部2は、共通鍵、または暗号鍵もしくは復号鍵などの鍵情報を用いたデータ変換を伴う所定のデータ処理を行う。所定のデータ処理としては、例えば、DESやFEALなどの共通鍵暗号方式あるいはRSAなどの公開鍵暗号方式等に基づいた、暗号化、復号化、デジタル署名などの認証データ生成、デジタル署名の署名検証などの認証データ検証などがある。ここでは、データ処理部2の処理内容はあらかじめ定められた1つのものであるとする。

【0028】より具体的な構成としては、このデータ処理部の処理内容が暗号化の場合、データ処理部は暗号化部などとなる。また、データ処理部の処理内容が復号化、認証データ生成あるいは認証データ検証などの場合も、それぞれ同様に、復号化処理部、認証データ生成部もしくは署名部、認証データ検証部もしくは検証部などとなる。

【0029】誤動作検出部3は、データ処理部2に対する入力データと、データ処理部2による処理結果のデータと、所定の鍵情報とをともに、データ処理部2に誤動作が生じたか否かを判断し、判断結果に応じて所定の制御信号を出力する。

【0030】誤動作検出部3で用いる鍵情報は、データ処理部2で用いる鍵情報に対応するものであり、データ処理部2の処理で用いる暗号方式やこの誤動作検出部3で用いる誤動作検出方式に応じて定まる。

【0031】誤動作検出方式としては、詳しくは後述するが、(1)データ処理部2と同一の処理を同一入力データに対して施し、得られた2つの処理結果が一致するか否かを比較する(一致しなかった場合に誤動作発生と判断する)もの、(2)データ処理部2の処理結果に対して逆変換処理を施し、この結果ともとの入力データが一致するか否かを比較する(一致しなかった場合に誤動作発生と判断する)ものなど、種々の方法が考えられる。

【0032】鍵保管部5は、データ処理部2にて用いる鍵情報と誤動作検出部3で用いる鍵情報を保管している。なお、鍵保管部5に、誤動作検出部3で用いるために、暗号化情報を受け渡しする相手側装置の秘密鍵が保管されている場合、この相手側装置の秘密鍵は、誤動作検出部3以外からはアクセスできないものとする。

【0033】出力制御部4は、誤動作検出部3によりデータ処理部2に誤動作が発生しなかったと判断された場合、データ処理部2の処理結果を外部に出力し、誤動作検出部3によりデータ処理部2に誤動作が発生したと判断された場合、データ処理部2の処理結果を外部に出力しないようにする。

【0034】この出力制御の方法としては、(1)誤動作検出部3は、誤動作を検出したときのみ誤動作検出信号を出力し、出力制御部4は、誤動作検出部3から誤動作検出信号が渡されたときのみ、処理結果を外部に出力せず、それ以外の場合は処理結果を出力する方法、

(2)誤動作検出部3は、誤動作を検出しなかったときのみ正常動作検出信号を出力し、出力制御部4は、誤動作検出部3から正常動作検出信号が渡されたときのみ、処理結果を外部に出力し、それ以外の場合は出力しない方法、(3)誤動作検出部3は、誤動作を検出しなかったとき正常動作検出信号を出力し、誤動作を検出したとき誤動作検出信号を出力し、出力制御部4は、誤動作検出部3から正常動作検出信号が渡されたときのみ、処理結果を外部に出力し、誤動作検出部3から誤動作検出信

号が渡されたときのみ、処理結果を外部に出力せず、何らかの理由でどちらの信号も渡されなかった場合、エラー処理（例えば、エラー回数が一定値になるまでは誤動作検出信号が与えられたものとみなし、エラー回数が一定値を越えたら当該タンパーフリー装置の機能自体を停止させるなど）を行う方法など、種々の方法が考えられる。

【0035】図2に、本実施形態に係るタンパーフリー装置の動作の流れを示す。処理対象となるデータ（例えばメッセージ）が入力されると、鍵保管部5に格納された鍵を使って、データ処理部2によりデータ変換処理がなされる（ステップS1）。

【0036】次に、誤動作検出部3は、データ処理部2の誤動作の有無を検出する（ステップS2）。データ処理部2の処理に誤動作はなかったと判断された場合（ステップS3）、処理結果は出力制御部4を介して外部に出力される（ステップS4）。

【0037】一方、データ処理部2の処理に誤動作が生じたと判断された場合（ステップS3）、処理結果は出力制御部4にて遮断され、外部への出力が禁止される（ステップS5）。

【0038】また、例えばデータ処理部2の機能が暗号化である場合には、タンパーフリー装置のより具体的な動作の流れは次のようになる。なお、復号化、認証データ生成あるいは認証データ検証などの場合も、それぞれ同様である。

【0039】暗号化対象となる平文メッセージなどのデータが入力されると、データ処理部（この場合、暗号部に相当）2は、鍵保管部5に格納された暗号鍵（もしくは共通鍵）を使って、このメッセージを暗号化する（ステップS1）。

【0040】次に、誤動作検出部3は、データ処理部2の暗号化処理に誤動作が発生したか否かを、平文データと暗号化データをもとにして検出する（ステップS2）。例えば、平文データの暗号化を再度実行して、両方の暗号化データが一致するか否かを調べる。あるいは、暗号化データを復号してもとの平文データに戻るか否かを調べる。

【0041】データ処理部2の暗号化処理に誤動作はなかったと判断された場合（ステップS3）、暗号化データは出力制御部4を介して外部に出力される（ステップS4）。

【0042】一方、データ処理部2の暗号化処理に誤動作が生じたと判断された場合（ステップS3）、暗号化データは出力制御部4にて遮断され、外部への出力が禁止される（ステップS5）。

【0043】さて、前述したような新しい暗号解析技術を用いて、タンパーフリー装置1の内部に隠された鍵情報などの秘密情報を暴こうとする者は、処理対象のデータを入力し、そしてデータ処理部3を誤動作させるため

に装置本体に放射線や電子パルス、磁気、熱、光等を当て、内部情報に依存した誤動作の影響が反映された出力データを観測しようとする。

【0044】しかしながら、本実施形態によれば、タンパーフリー装置1に放射線等が当てられデータ処理部3に誤動作が生じた場合、誤動作検出部3の働きにより、誤動作の影響を反映した処理結果が外部に出力されることが禁止される。この結果、攻撃者は、誤動作が生じた場合の出力データを得ることはできず、タンパーフリー装置1内部の秘密情報を暴くことはできない。

【0045】このように、本実施形態に係るタンパーフリー装置1は、タンパーフリー装置自体に物理的衝撃を与え誤動作を起こさせて暗号解読しようとする新しい暗号解析技術に対し、簡易な構成で確実に対抗できる点で、非常に優れたものとなっている。

【0046】以下では、図1で説明した構成を発展させたものやより具体化したものなどについて幾つかの例を示す。図3は、図1の構成において、誤動作検出部3による検出結果を示す制御情報を外部に出力するようにしたものである。この場合、制御情報の出し方には幾つかのものが考えられる。

【0047】例えば、誤動作検出部3は、誤動作がなかったと判断された場合にのみ、誤動作がないことを示す信号を出力するようにしても良い。あるいは、誤動作があったと判断された場合にのみ、誤動作があったことを示す信号を出力するようにしても良い。あるいは、誤動作がなかったと判断された場合に、誤動作がないことを示す信号を出力し、誤動作があったと判断された場合に、誤動作があったことを示す信号を出力するようにしても良い。

【0048】図4は、図1の構成において、鍵保管部5に複数の鍵をID番号と対応付けて格納しておき、データ処理部2の処理で用いる鍵を外部から指定可能にしたものである。なお、データ処理部2で用いる鍵と、誤動作検出部3で用いる鍵が異なる場合、例えば、データ処理部2で暗号鍵を用いて暗号化し、誤動作検出部3でこの暗号鍵とは異なる復号鍵を用いて復号化するような場合、両方の鍵を対応付けて格納しておく。

【0049】このようにした場合、処理対象となるデータの入力の前もしくは同時もしくは後に、使用する鍵のID番号を指示入力する。データ処理部2や誤動作検出部3は、指示されたID番号に対応する鍵を用いて処理を行う。

【0050】図5は、図1の構成において、データ処理部2が複数の種類のデータ処理を実行可能とし、データ処理部2の処理内容の種類を外部から指定可能にしたものである。

【0051】データ処理内容の組み合わせは任意であるが、具体例としては次のようなものがある。

(1) 幾つかの異なる方式の暗号化機能を備えるケース

- (2) 幾つかの異なる方式の復号化機能を備えるケース
- (3) 幾つかの異なる方式の認証データ生成機能を備えるケース
- (4) 幾つかの異なる方式の認証データ検証機能を備えるケース
- (5) 1または複数の対の暗号化機能と復号化機能を備えるケース
- (6) 1または複数の対の認証データ生成機能と認証データ検証機能を備えるケース
- (7) 1または複数の対の暗号化機能と復号化機能、および1または複数の対の認証データ生成機能と認証データ検証機能を備えるケース

なお、処理に応じて異なる鍵を用いることがある場合、処理のID番号とその処理で使用する鍵とを対応付けて鍵保管部5に格納しておく。

【0052】図6に、図5のように構成したタンパーフリー装置の動作の流れを示す。まず、実行すべきデータ処理の内容を示すID番号を入力する(ステップS21)。

【0053】例えばデータ処理部2の機能が暗号化または復号化であり、暗号化処理を指示する場合には、暗号化処理のID番号を入力する(ステップS21)。ステップS21の入力の前もしくは同時もしくは後に処理対象となるデータ(例えばメッセージ)が入力されると、鍵保管部5に格納された鍵を使って、データ処理部2によりデータ変換処理がなされる(ステップS22)。

【0054】次に、誤動作検出部3は、データ処理部2の誤動作の有無を検出する(ステップS23)。データ処理部2の処理に誤動作はなかったと判断された場合(ステップS24)、処理結果は出力制御部4を介して外部に出力される(ステップS25)。

【0055】一方、データ処理部2の処理に誤動作が生じたと判断された場合(ステップS24)、処理結果は出力制御部4にて遮断され、外部への出力が禁止される(ステップS26)。

【0056】なお、図3で説明した誤動作検出部5が検出結果を示す制御情報を外部に出力する構成、図4で説明した外部から鍵の指定を可能とする構成、図5で説明した外部から処理内容の指定を可能とする構成は、任意に組み合わせることが可能である。

【0057】例えば、図4と図5を組み合わせ、外部から鍵の指定を可能とするとともに、処理内容の指定を可能とする場合、鍵保管部5に複数の鍵(または暗号鍵と復号鍵の対)を鍵ID(または鍵IDおよび処理ID)と対応付けて格納しておき、処理対象となるデータの入力の前もしくは同時もしくは後に、処理IDと鍵IDを指示入力するようにすればよい。

【0058】以下では、誤動作検出部3のより具体的な例について説明する。前述したように誤動作検出方式としては、主として、(1)データ処理部2と同一の処理

を同一入力データに対して施し、得られた2つの処理結果が一致するか否かを比較する(一致しなかった場合に誤動作発生と判断する)もの、(2)データ処理部2の処理結果に対して逆変換処理を施し、この結果ともの入力データが一致するか否かを比較する(一致しなかった場合に誤動作発生と判断する)ものが考えられる。

【0059】ここで、説明の便宜上、(1)の方法を2重化法、(2)の方法を検算法と呼ぶ。データ処理部2の処理内容にかかわらず2重化法は常に適用可能であるが、検算法はデータ処理部2の処理内容に依存して適用可能な場合と適用不可の場合がある。

【0060】データ処理部2の処理内容として検算法が適用可能なものは、例えば以下のような処理である。

(a) ある処理とその逆変換処理で同一の鍵を用いるもの

(b) 公開鍵暗号方式に基づく可逆な処理で、検算処理に相手側の秘密鍵が不要なもの

(c) 公開鍵暗号方式に基づく可逆な処理でかつ検算処理に相手側の秘密鍵を必要とするものであって、相手側の秘密鍵が当該誤動作検出のために使用可能な場合

なお、データ処理部2の処理が不可逆の処理(例えばDSA)である場合、検算法を適用することはできない。

【0061】(a)の具体例としては、共通鍵暗号方式に基づく暗号化と復号化(例えばDES、FEAL)が該当する。

(b)の具体例としては、公開鍵暗号方式に基づく復号化、公開鍵暗号方式に基づく認証データ生成で可逆なもの(例えばRSA)が該当する。

【0062】(c)の具体例としては、公開鍵暗号方式に基づく暗号化、公開鍵暗号方式に基づく認証データ検証で可逆なもの(例えばRSA)が該当する。

図7に、図1～図6を用いて説明したタンパーフリー装置の誤動作検出部3の構成に2重化法を用いた場合の一例を示す。

【0063】データ処理部31は、データ処理部2と同一の処理機能を持つものである。比較部32は、データ処理部2の出力とデータ処理部31の出力を比較し、前述したように比較結果に応じて所定の制御信号を出力する。

【0064】ここで、データ処理部2とデータ処理部31とは、回路を独立させて、互いの処理を同時実行可能にすれば、誤動作検出処理に要する時間を大幅に削減することができる。

【0065】なお、誤動作検出処理に要する時間が多少かかっても、回路量を削減したい場合には、データ処理部2とデータ処理部31を1つの回路で共用するように構成してもよい。

【0066】図8に、図1～図6を用いて説明したタンパーフリー装置の誤動作検出部3の構成に検算法を用いた場合の一例を示す。逆変換部33は、データ処理部2

13

で行う処理に対する逆変換処理の機能を持つものである。比較部32は、データ処理部2の出力と逆変換部33の出力を比較し、前述したように比較結果に応じて所定の制御信号を出力する。

【0067】ここで、誤動作検出処理による全体の処理性能の低下を防ぐために、暗号化処理と誤動作検出処理を並列化してもよい。例えば、データ処理部2と逆変換部33とで回路を独立させ、これにパイプライン処理を適用すれば、誤動作検出処理に要する時間を大幅に削減することができる。

【0068】例えば図9に示すように、データ処理部2で暗号化を行い、逆変換部33で復号化を行う場合、入力ブロック#1は、暗号化された後、誤動作検出(検算)のために復号される。一方、このブロック#1の復号が行われている間、次のブロック#2の暗号化が行われる。これによって、1つのブロックが入力されてから出力が得られるまで2単位時間の遅延がかかるだけで、誤動作検出処理を行わない場合と略同様の処理性能を得ることができる。

【0069】なお、データ処理部2と逆変換部33の構成が同一になる場合には、誤動作検出処理に要する時間が多少かかっても、回路量を削減したいならば、データ処理部2と逆変換部33を1つの回路で共用するように構成してもよい。

【0070】以下では、図1～図6を用いて説明したタンパーフリー装置のデータ処理部2の処理がラウンド関数を用いる場合の構成例について説明する。DESやFEALのようなラウンド関数を用いる暗号アルゴリズムでは、暗号化したい平文に対し、鍵をパラメータとするラウンド関数を繰り返し適用する。例えば、4段の変換を用いる場合、まず平文は第1のラウンド関数により変換され、変換結果は第2のラウンド関数により変換され、この変換結果がさらに第3のラウンド関数と第4のラウンド関数により順次変換される。暗号アルゴリズムによって、ラウンド関数の段階数が定められる。復号化についても同様である。

【0071】ところで、このようなラウンド関数を積み重ねた積暗号方式では、各ラウンド毎に誤動作検出を行うことが可能である。そこで、例えば暗号化の場合、もとの暗号化回路の他に、誤動作検出のための暗号化回路(2重化法の場合)あるいは復号化回路(検算法の場合)を独立して持ち、並列演算を行うことにより、誤動作検出処理による全体の処理速度の増大を防ぐことが可能となる。つまり、あるラウンド関数の処理結果をもとに誤動作検出処理を実行すると同時に後続するラウンド関数の暗号化処理(あるいは復号化処理)を行うことができる。そして、あるラウンド関数の処理に誤動作が生じたと判断された場合、その時点で処理を停止させ、あるいは最終的な処理結果が外部に出力されるのを禁止させることができる。

14

【0072】図10に、ラウンド数が4段で、かつ誤動作検出部3の構成に2重化法を用いた場合の一例を示す。暗号化回路201～204、301～304は、それぞれラウンド関数に対応する。

【0073】比較部311～314では、2つの暗号化されたデータを比較し、その結果を動作制御部321に通知する。動作制御部321は、比較部311～313から誤動作検出の通知を受けた場合、次段以降の処理を停止させ、最終段の比較部314から誤動作検出の通知を受けた場合、出力制御部4を制御して最終的な処理結果が外部に出力されないようにする。

【0074】なお、復号化を行う場合も、同様の構成である。図11に、ラウンド数が4段で、かつ誤動作検出部3の構成に検算法を用いた場合の一例を示す。

【0075】暗号化回路201～204は、それぞれラウンド関数に対応する。復号化回路331～334は、それぞれ対応する暗号化回路201～204の逆関数を実行する。

【0076】比較部311～314では、対応する暗号化回路201～204への入力データと、対応する復号化回路331～334の処理結果を比較し、その結果を動作制御部321に通知する。

【0077】動作制御部321は、比較部311～313から誤動作検出の通知を受けた場合、次段以降の処理を停止させ、最終段の比較部314から誤動作検出の通知を受けた場合、出力制御部4を制御して最終的な処理結果が外部に出力されないようにする。

【0078】なお、復号化を行う場合も、同様の構成である。図12に、図10と図11のタンパーフリー装置の処理の流れを示す。まず、データ処理部2における第1段のラウンド関数を実行する(ステップS31)。なお、図10の構成の場合、誤動作検出部3における第1段のラウンド関数を同時に実行できる。

【0079】次に、データ処理部2における第2段のラウンド関数を実行するとともに(ステップS32)、第1段のラウンド関数の実行についての誤動作検出処理を行う(ステップS33)。なお、図11の構成の場合、誤動作検出部3における第1段のラウンド関数を実行した後に、比較部311での比較処理を行う。

【0080】誤動作が検出された場合(ステップS34)、ラウンド関数の実行を停止させる処理が実行される(ステップS35)。誤動作が検出されなかった場合(ステップS34)、そのままラウンド関数の実行は継続される。

【0081】以降、このような動作が最終段(ここでは4段目)まで繰り返される(ステップS36～S43)。そして、最終段の誤動作検出処理が実行され(ステップS44)、誤動作が検出された場合(ステップS45)、最終的な処理結果の外部への出力は禁止される(ステップS46)、誤動作が検出されなかった場合

15

(ステップS45)、最終的な処理結果が外部へ出力される(ステップS47)。

【0082】なお、図10～図12では、ラウンド数が4段である場合について説明したが、もちろん、本構成は、所望のラウンド数のものに適用可能である。ところで、図10や図11の構成において、ラウンド対応部分を1組の回路で共用し、回路量を削減することも可能である。

【0083】そのような構成の一例として、図13に、データ処理部2と誤動作検出部3の両方で暗号化を行う場合の構成例を示す。また、図14に、データ処理部2で暗号化を行い、誤動作検出部3で復号化を行う場合の構成例を示す。伝える。

【0084】選択回路211は、外部からのデータ入力時には、入力データを暗号部201側に伝え、その他ではラウンド関数の実行のために、選択回路212の出力を伝える。

【0085】選択回路212は、最終段のラウンド関数の実行までは、暗号部201の出力を選択回路211に伝え、最終段のラウンド関数の実行結果は、出力制御部4に伝える。

【0086】以下では、これまで説明してきた各実施形態の変形例を幾つか示す。各実施形態では、誤動作を検出したら外部への出力を禁止するものであったが、その代わりに、誤動作を検出したら、再度計算を繰り返すようにしても良い。また、この場合に、その繰り返しが一定数を越えたら、装置自体を所定の方法でロックして使用できなくするようにしても良い。あるいは、繰り返しが一定数を越えた場合に、その旨を示す信号を外部に出力するようにしても良い。

【0087】また、誤動作を検出したら、外部にデータを出力しない代わりに、乱数を出力するようにしても良い。この場合、出力データを全て乱数に置き換えても良いし、装置内部の秘密情報の反映を解消できる程度で、出力データの一部のみ乱数に置き換えても良い。

【0088】また、RSA暗号方式を用いる場合、パラメータ e を小さくすることにより、復号化に対する検算(暗号化)時間を短くしても良い。ところで、前述した暗号化回路などのデータ処理部を2重化することにより誤動作を検出する方式において、同じ役割を果たす2重化された2つの回路の配線が互いに隣り合わず、物理的に離れているようなレイアウトに配置すると好ましい。

【0089】例えば、図15では、半導体基板340上で、第1の暗号化回路341と、第2の暗号化回路343とを、比較回路342を挟んで、物理的に距離をあけて配置させた様子を示している。

【0090】暗号解読のために誤動作を起こさせようとタンパーフリー装置自体に外部より物理的衝撃を加える際に、放射線を焦点を絞って照射することが困難であるなど、物理現象をスポット的に生じさせることが困難で

16

ある場合、上記のようにすることで、2重化された2つの回路で誤動作の生じる箇所を互いに異ならせるようにし、偶然に2つの回路で同一の誤動作が発生し、比較回路で誤動作が見過ごされるようなことをほぼ完全に回避することができる。

【0091】以上では、タンパーフリー装置内で、1種類の処理を施す例を示してきたが、複数の処理、例えば、暗号化と電子署名の2つの処理(あるいは復号化と電子署名検証)を連続して行うようにしても良い。その際、複数の処理の少なくとも1つに誤動作が検出された場合、すべての処理について外部へのデータ出力を禁止する方法や、誤動作が検出された処理についてのみ外部へのデータ出力を禁止する方法などが考えられる。

【0092】次に、本発明の第2の実施形態に係るタンパーフリー装置について説明する。これまで説明してきた第1の実施形態は、概略的には、処理にあたっての誤動作を検出したら処理結果の出力を禁止するものであった。

【0093】この第2の実施形態は、誤動作の有無は判断せず、処理結果も常に出力することとし、その代わりに、誤動作の結果得られる出力データに内部状態が反映されないように工夫したものである。

【0094】図16に、本実施形態にかかるタンパーフリー装置の内部機能の一例を示す。401は、この処理におけるもともとの変換 E を実行するデータ処理部である。例えば、変換 E は、暗号化あるいは復号化に該当する。

【0095】402は、変換 E の逆変換 E^{-1} を実行する逆変換部である。403と406は、同一の所定の演算を行う演算部である。この所定の演算を示す演算子を記号 \bigcirc で表すこととする。

【0096】404は、所定の方法で乱数 R を発生する乱数発生部である。405は、乱数 R の逆元 R^{-1} を求める逆元処理部である。なお、404と405を一体化させて、乱数 R とその逆元 R^{-1} を同時に求めても良い。

【0097】ここでは、排他的論理和など所定の演算子 \bigcirc に対して、 $E(A \bigcirc B) = E(A) \bigcirc E(B)$ が成立する準同型性を持つ暗号化関数を使用する暗号(例えばRSA暗号)を考える。

【0098】なお、 $C \bigcirc a = C$ となる場合に、 D に対して、 $D \bigcirc D^{-1} = a$ とする D^{-1} を、 R の逆元と呼び、 R の逆元 R^{-1} を求める処理を、逆元処理と呼ぶ。例えば、演算子 \bigcirc が排他的論理和を表す場合、 $a = 1$ であり、演算子 \bigcirc が排他的論理積を表す場合、 $a = 0$ である。

【0099】さて、準同型性を持つ暗号化関数を使用する暗号では、乱数 R を逆変換 E^{-1} した結果 $E^{-1}(R)$ を求め、暗号化対象となる平文 M と $E^{-1}(R)$ に演算 \bigcirc を施した結果 $M \bigcirc E^{-1}(R)$ を求め、この $M \bigcirc E^{-1}(R)$ を変換 E した結果 $E(M \bigcirc E^{-1}(R))$ を求め、また、上記の乱数 R の逆元 R^{-1} を求め、 $E(M \bigcirc E^{-1}(R))$

17

とR-1に演算○を施した結果E (M) ○E (E⁻¹ (R)) ○R-1を求めると、これが平文Mを変換Eした結果E (M) に等しいという性質がある。

【0100】すなわち、E (M○E⁻¹ (R)) ○R-1
 = E (M) ○E (E⁻¹ (R)) ○R-1
 = E (M) ○R○R-1
 = E (M)
 となる。

【0101】本実施形態では、このような演算過程で乱数を混入させるという操作を行ったにもかかわらず結果は乱数に依存せず一定であるという性質を利用している。すなわち、変換Eの処理中に発生した誤動作の影響は、乱数Rを混入させることにより拡散され、暗号解読に役立つ情報を得ることができなくなる。この操作は、物理的手段により誤動作を誘発させて暗号を解読しようとする新たな攻撃法に対して絶大な効果がある。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0102】

【発明の効果】本発明によれば、タンパーフリー装置の内部回路が誤動作した場合、処理結果をデータ出力しないので、外部から物理的衝撃を加えて内部回路を誤動作させその出力を観察して装置内部の秘密情報を暴こうとする攻撃を阻止することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態にかかるタンパーフリー装置の一構成例を示す図

【図2】同実施形態に係るタンパーフリー装置の動作の流れの一例を示すフローチャート

【図3】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図4】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図5】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図6】同実施形態に係るタンパーフリー装置の動作の *

18

*流れの他の例を示すフローチャート

【図7】誤動作検出部の一例を示す図

【図8】誤動作検出部の他の例を示す図

【図9】パイプライン処理による高速化を説明するための図

【図10】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図11】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

10 【図12】同実施形態に係るタンパーフリー装置の動作の流れの他の例を示すフローチャート

【図13】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図14】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図15】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

【図16】同実施形態にかかるタンパーフリー装置の他の構成例を示す図

20 【符号の説明】

1…タンパーフリー装置

2, 401…データ処理部

3…誤動作検出部

4…出力制御部

5…鍵保管部

31…データ処理部

32…比較部

33, 402…逆変換部

201~204, 301~304…暗号化回路

30 311~314…比較部

321…動作制御部

331~334…復号化回路

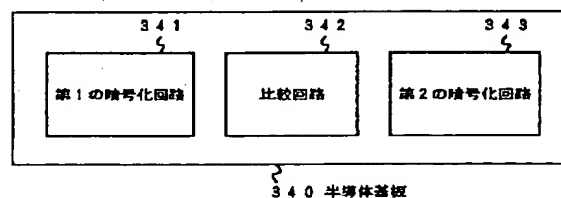
211, 212…選択回路

403, 406…演算部

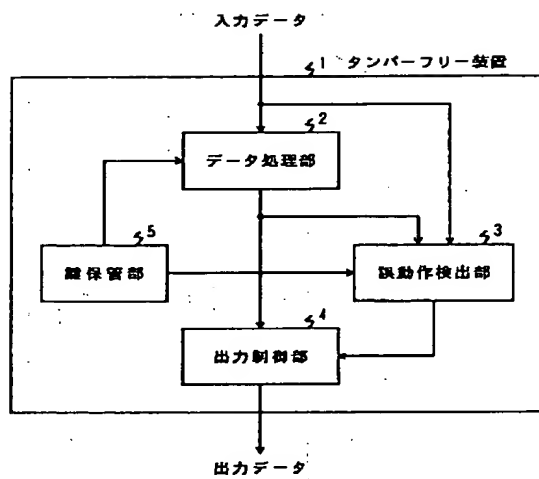
404…乱数発生部

405…逆元処理部

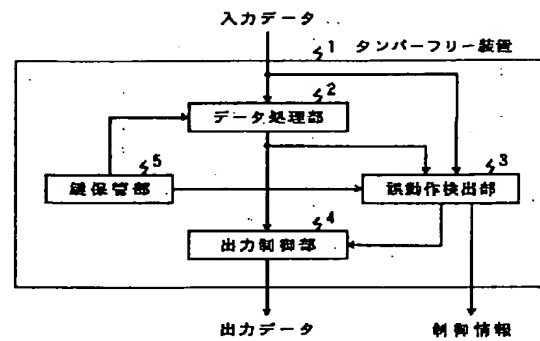
【図15】



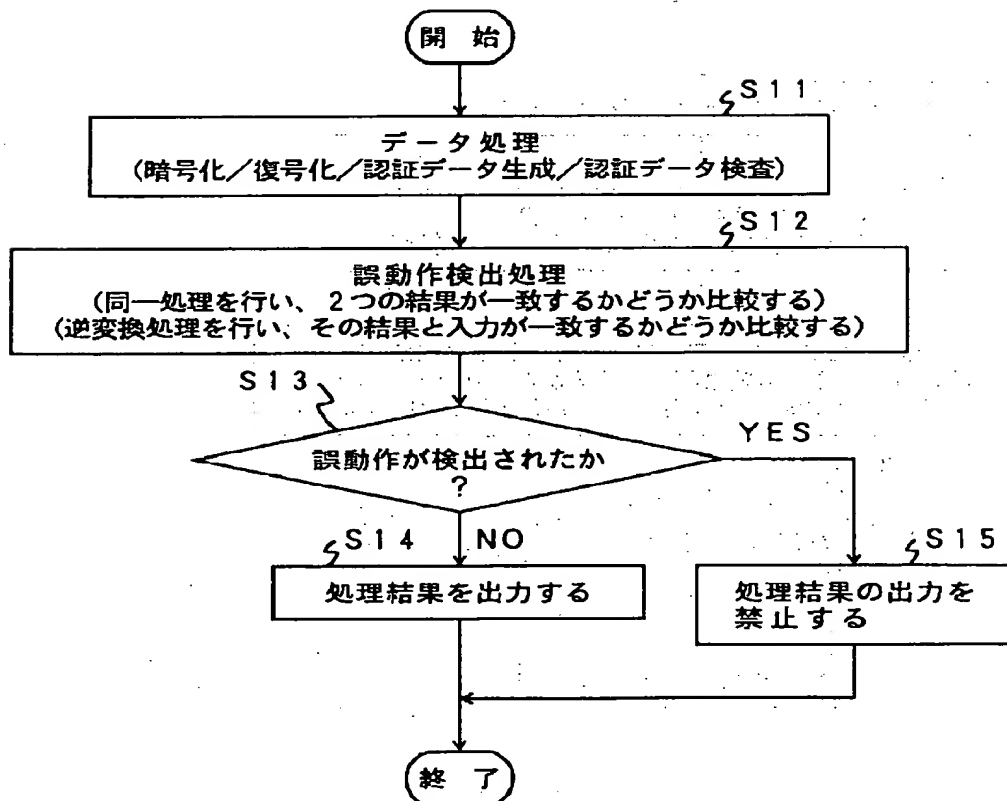
【図1】



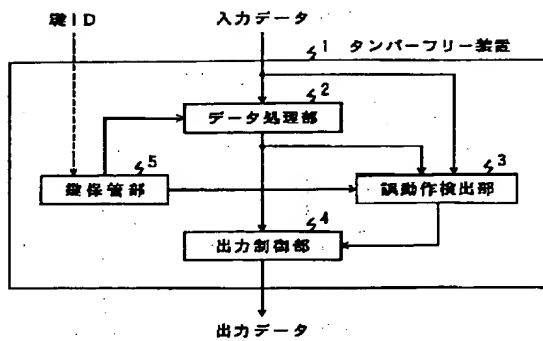
【図3】



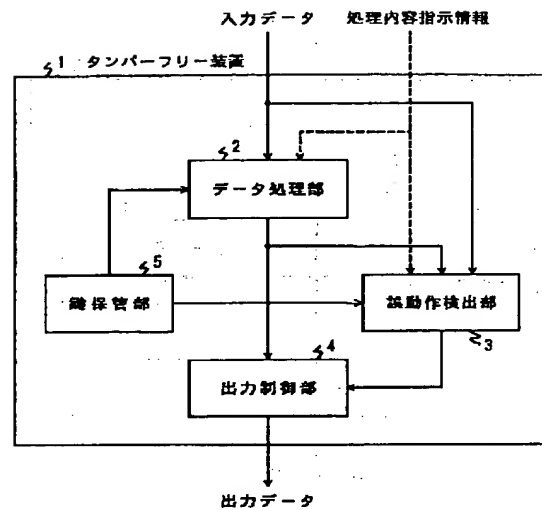
【図2】



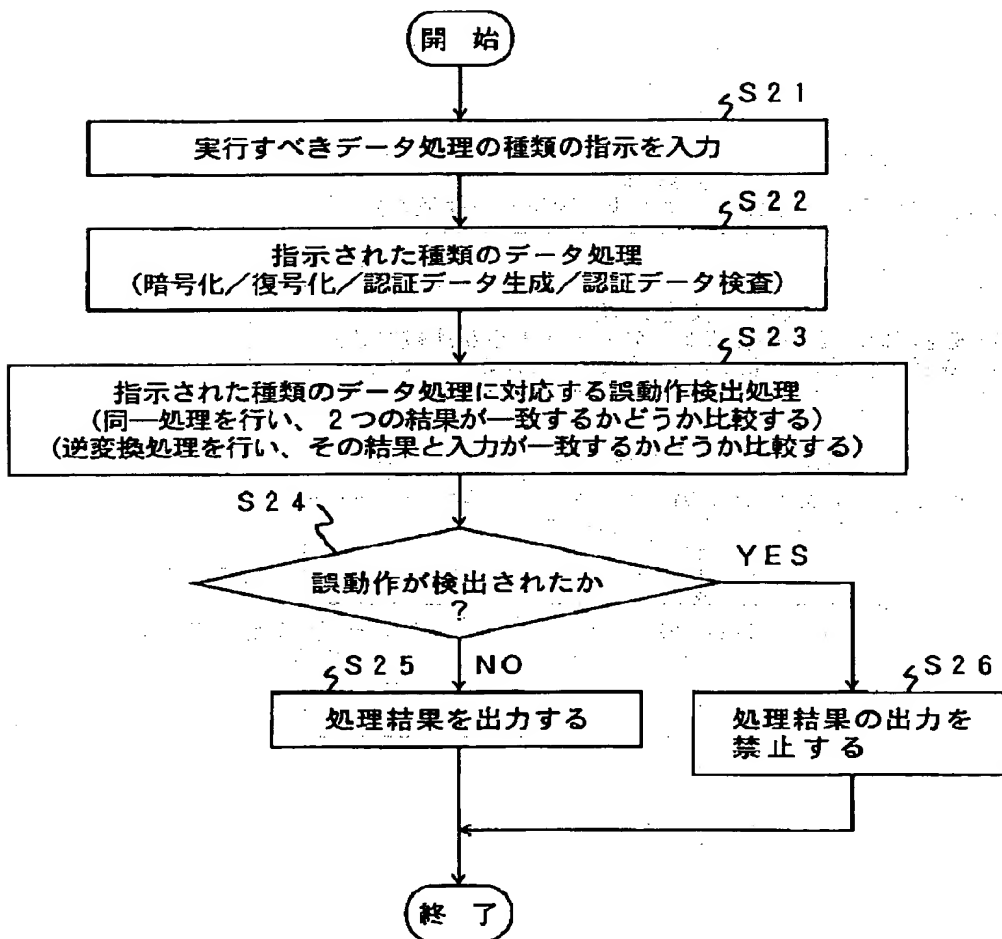
【図4】



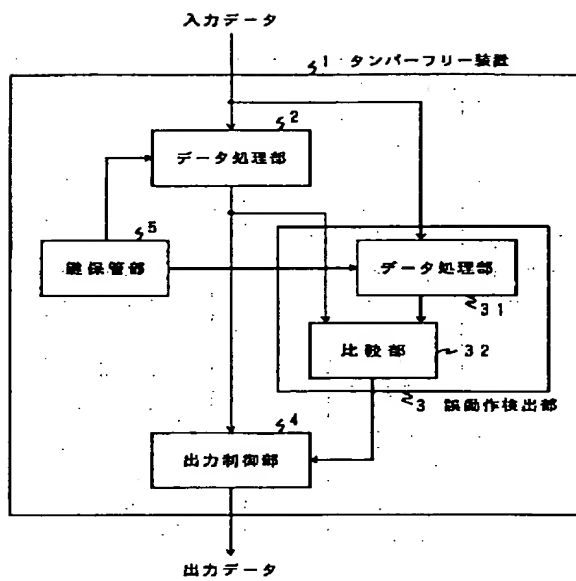
【図5】



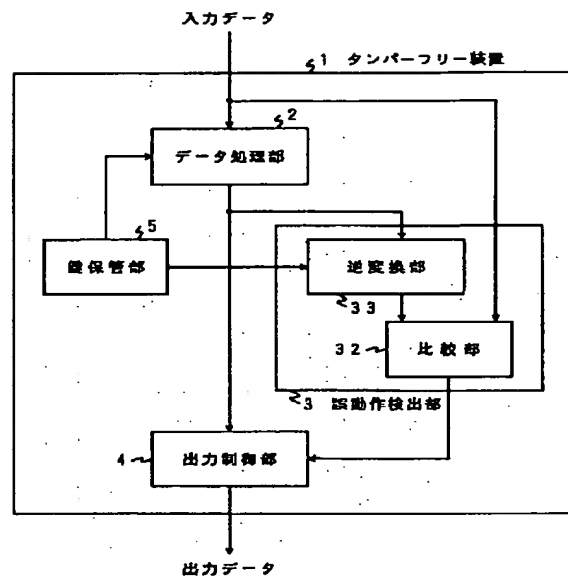
【図6】



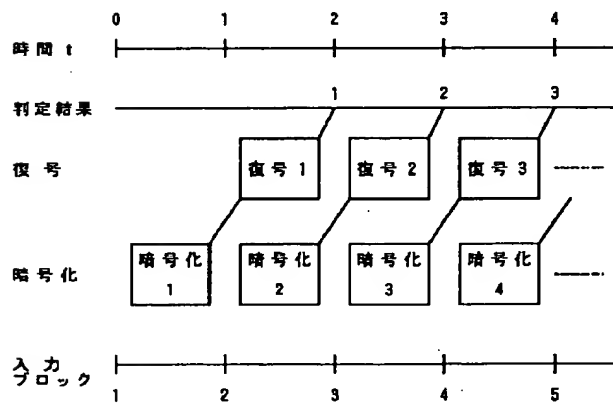
【図 7】



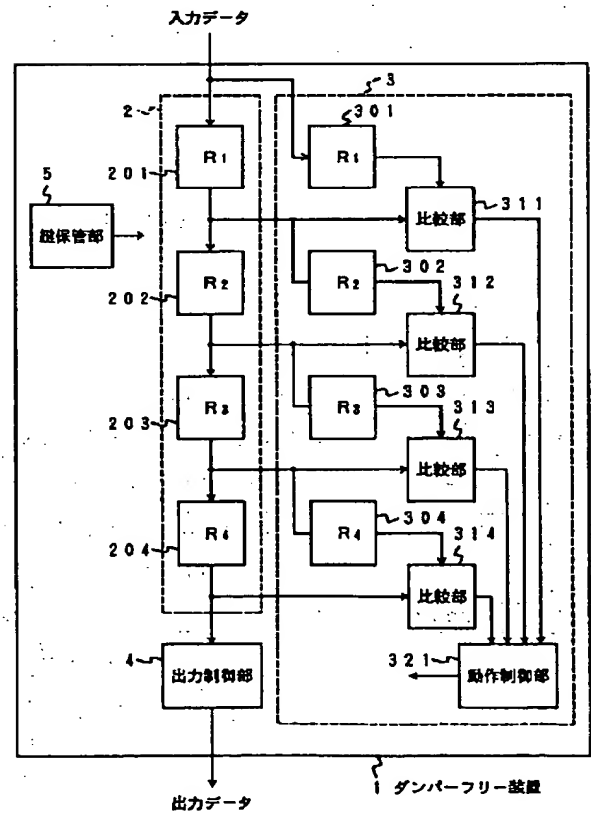
【図 8】



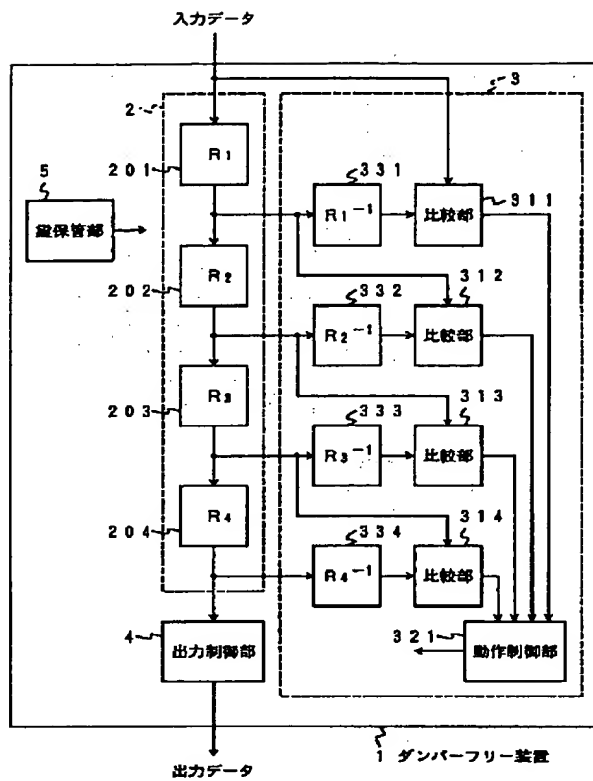
【図 9】



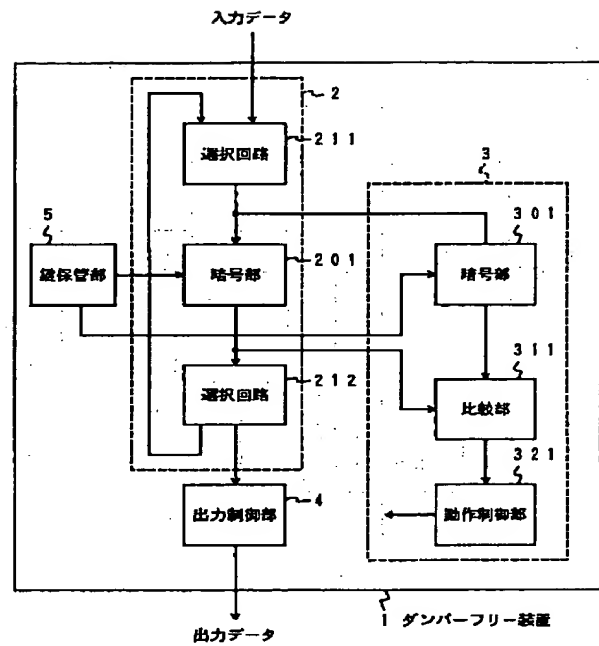
【図 10】



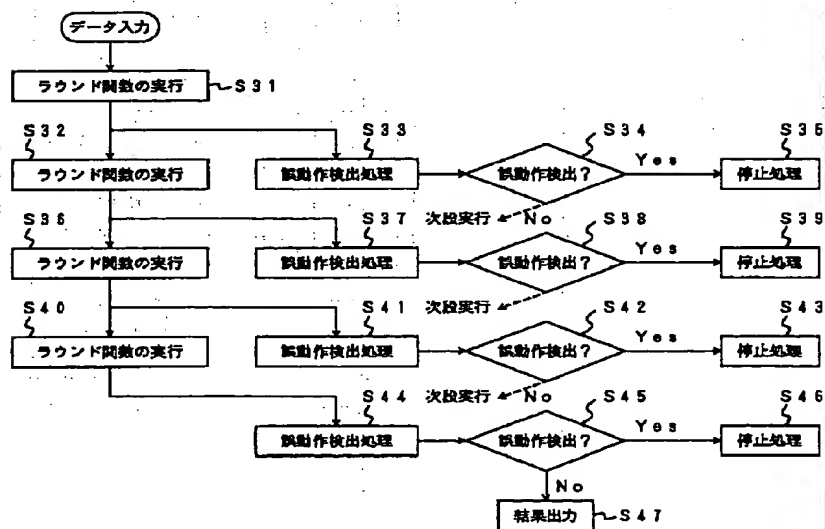
【図 11】



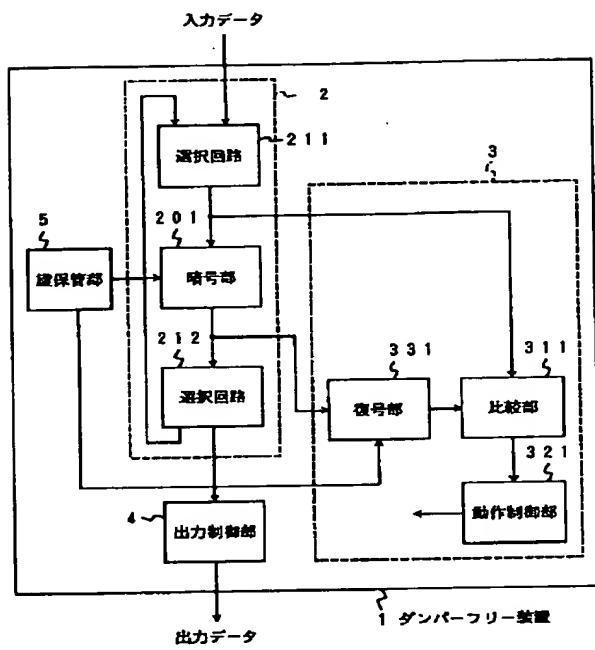
【図 13】



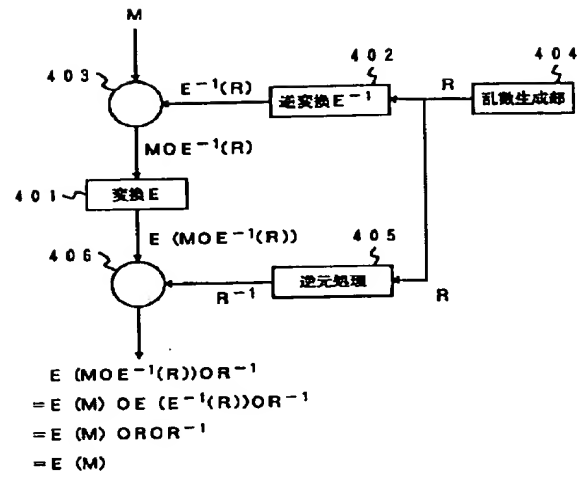
【図 12】



【図 14】



【図 16】



THIS PAGE BLANK (USPTO)